Exhibit 28

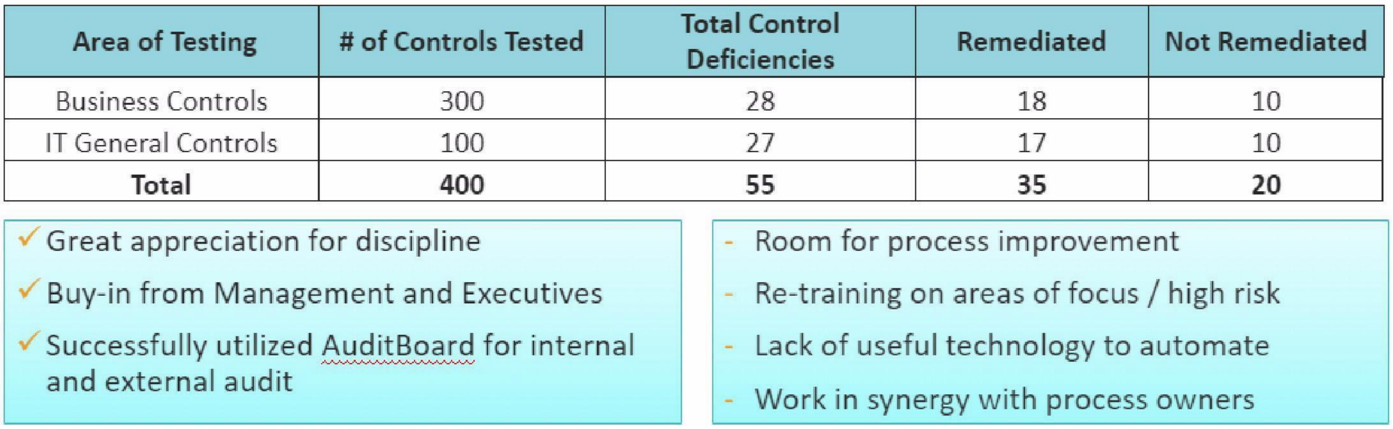
Excerpts of SW-SEC00388330

From: Campbell, Danielle [/O=EXCHANGELABS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=BF58A9FD896640A592DDD2AF5D6DA453-CAMPBELL, D]
Sent: 3/2/2020 9:11:47 PM
To: Ensminger, Sandy [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=05e9c9c023b449b794de995f6362b10d-Ensminger,]; Day, Chris [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=aa9a0d2c87114c0898a128020a311291-Day, Chris]; Wehrmann, August [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=73ef7e48062645d5be3af7b9068c1f15-Wehrmann, A]; Kemmerer, Joel [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=7001182857294219b50223772a1dd507-Kemmerer, J]; Owens, David [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=a4c0c534892740c8b2af623237debff0-Owens, Davi]
CC: Johnson, Rani [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=0ee57945f15e47b3abaa99a59170ad3f-Johnson, Ra]
Subject: SOX: Control Deficiencies FY19
Attachments: FY2019 Deficiencies and Recommendations - Final.xlsx

Hi –

I wanted to send you an email to let you know that we have control deficiencies from our FY19 SOX Audit that will need to be remediated by your teams. I have set up meetings with the control owners over the next couple of weeks. The goal of these meetings will be to determine what remediation steps will be taken and how quickly they can be put in place. I believe that most of the remediation efforts will be around re-training the teams on the process that should be followed for financially impacting changes. I don't believe that there will need to be any work around these unless the teams decide the old process will not work and need to be changed.

Attached is a summary of all the control deficiencies for both business and IT controls. There were 20 controls that were not remediated by yearend. I would like to have all of these remediated in Q1 or early Q2. If you filter on column K, the focus will be on those that have not been remediated yet. Majority of the teams are already aware of these since they were heavily involved in the discussions with Internal Audit and PwC. Just in case they did not make it to you, I wanted to present them to you. (the IT controls are on the last tab)



Area of Testing	# of Controls Tested	Total Control Deficiencies	Remediated	Not Remediated
Business Controls	300	28	18	10
IT General Controls	100	27	17	10
Total	**400**	**55**	**35**	**20**

- ✓ Great appreciation for discipline
- ✓ Buy-in from Management and Executives
- ✓ Successfully utilized AuditBoard for internal and external audit

- Room for process improvement
- Re-training on areas of focus / high risk
- Lack of useful technology to automate
- Work in synergy with process owners

We have the Security & Compliance Quarterly Risk Review (QRR) meeting tomorrow with Jason Bliss and Bart Kalsu. We have a couple slides dedicated to the SOX findings. I did not want it to be a surprise to you that these are included in that discussion.

Please let me know if you have any questions or if you would like for me to have a separate call with you to review. I have already included you on the meeting invites with your teams to review these as well.

Overall, for our first year as a public company, I believe the teams did a good job. However, we do have areas for improvement around these controls.

Thanks,

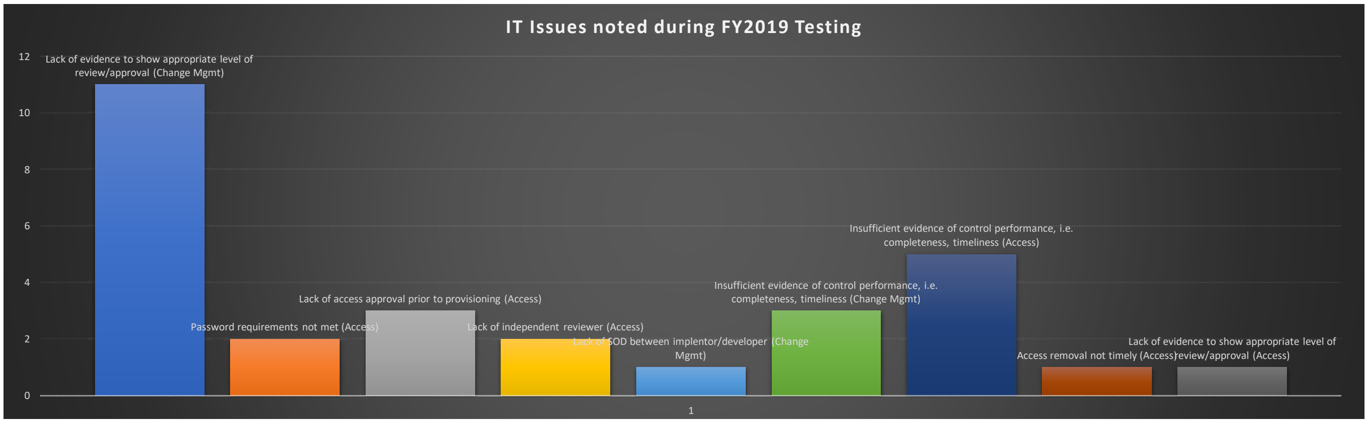
solarwinds

Danielle Campbell | Director of Internal Audit

Office: 512.874.3389 | Mobile: 972.467.8926

DOCUMENT PRODUCED IN NATIVE FORMAT

IT General Controls	Total
Lack of evidence to show appropriate level of review/approval (Change Mgmt)	11
Password requirements not met (Access)	2
Lack of access approval prior to provisioning (Access)	3
Lack of independent reviewer (Access)	2
Lack of SOD between implentor/developer (Change Mgmt)	1
Insufficient evidence of control performance, i.e. completeness, timeliness (Change Mgmt)	3
Insufficient evidence of control performance, i.e. completeness, timeliness (Access)	5
Access removal not timely (Access)	1
Lack of evidence to show appropriate level of review/approval (Access)	1
	29



#	Identified by PwC or Management	System	Process	Control Number	Control Language	Control Owner	Issue Short Name	Description of Control Deviation Identified by IA	Exception Type	Remediated	Mitigating Control #s	Why the impact is not pervasive?	Follow-up / Management Response / Action Plan	Period control not operating effectively
7	Holtzman/PWC	Backup	User Access Management	2.1	The Company maintains password requirements for all financially significant systems and databases, including the requirements that they be changed periodically, meet minimum length requirements, retain password history, and require password complexity, as allowed by the application, system, or database. Web hosted applications may not require active directory authentication. If access is limited by a password and requires log in into Active Directory (includes system accounts) the requirements for password change, password complexity and password history are not considered necessary.	Wood / Stuart Qui	Password requirements not met (Access)	Backup appears to utilize TUL / AD first and foremost. However, application guidance notes that, in instances where TUL / AD is not a possibility, the application-specific password policy is used. Per inspection of the Backup policy, only a portion of the password requirements are met – (1) complexity is enabled and (2) minimum characters are defined. However, (3) a maximum password age is not configured as required, nor is (4) a password history requirement.	CD	N	Control 2.5 - User Access Revi	The primary access path for Backup is through TUL / AD. Instances in which users are logging in outside of TUL / AD is not nearly as common and thus plays a role in limiting the risk found in the exception. Additionally, the application-specific password configuration detail meets some of the requirements, but not all, meaning there is security in the application-specific password detail just not to the extent that the control language requires. Lastly, the quarterly user access review performed over Backup provides comfort over restricted access.	Low Risk - this will be remediated in Q1 based on discussion with Oli Wood.	1/1/2019 - 12/31/2019
25	Holtzman/PWC	RMM	User Access Management	2.1	The Company maintains password requirements for all financially significant systems and databases, including the requirements that they be changed periodically, meet minimum length requirements, retain password history, and require password complexity, as allowed by the application, system, or database. Web hosted applications may not require active directory authentication. If access is limited by a password and requires log in into Active Directory (includes system accounts) the requirements for password change, password complexity and password history are not considered necessary.	Wood / Stuart Qui	Password requirements not met (Access)	RMM appears to utilize TUL / AD first and foremost. However, application guidance notes that, in instances where TUL / AD is not a possibility, the application-specific password policy is used. Per inspection of the RMM policy, only a portion of the password requirements are met – (1) complexity is enabled and (2) minimum characters are defined. However, (3) a maximum password age is not configured as required, nor is (4) a password history requirement.	CD	N	Control 2.5 - User Access Revi	The primary access path for RMM is through TUL / AD. Instances in which users are logging in outside of TUL / AD is not nearly as common and thus plays a role in limiting the risk found in the exception. Additionally, the application-specific password configuration detail meets some of the requirements, but not all, meaning there is security in the application-specific password detail just not to the extent that the control language requires. Lastly, the quarterly user access review performed over RMM provides comfort over restricted access.	Low Risk - this will be remediated in Q1 based on discussion with Oli Wood.	1/1/2019 - 12/31/2019
28	Internal Audit	Data Foundry	Access Provisioning	N/a	Control 6.16 Password requirements have also been established for Data Foundry servers and network devices, including password complexity and minimum length requirements. Control 6.12: User access management follows a formal process, which includes approval by the manager responsible for the applicable system within the Company.	Tim Brown	Insufficient evidence of control performance, i.e. completeness, timeliness (Access)	Exception Noted: For 2 servers (both running the Solaris OS) of 4 servers tested, password complexity was not enforced. Exception Noted: For 1 of 2 access changes tested, the access being requested, and that was approved, was not explicitly documented in the request.	CD	Y	N/a	Although password complexity was not set, other components of a secure password were configured, lowering the risk of inappropriate access to the servers. Since the access provisioned was requested and approved, this is a documentation error and is therefore low risk. No negative impact to the SolarWinds control environment expected.	Although password complexity was not set, other components of a secure password were configured, lowering the risk of inappropriate access to the servers. Since the access provisioned was requested and approved, this is a documentation error and is therefore low risk. No negative impact to the SolarWinds control environment expected.	
29	Internal Audit	Sungard	Access Provisioning	N/a	Control 4.6 Upon the termination of a SunGard AS employee, HR contacts various responsible functions that manage logical security to notify them that an individual has been terminated and access to SunGard AS Global Management Network is subsequently removed in a timely manner. Control 4.7: Access to SunGard AS Global Management Network is reviewed quarterly to validate that access is limited to individuals whose job responsibilities require such access rights.	Tim Brown	Insufficient evidence of control performance, i.e. completeness, timeliness (Access)	Exception Noted: Through inspection of the full population of 535 terminated users, determined that logical access rights were not removed in a timely manner for 4 terminated users. Through inquiry and inspection of evidence for the terminated users, determined logical access rights were subsequently removed and each user did not login to the SunGard AS network and underlying applications post-termination date. Exception Noted: Through inspection of the Q4 2018, Q1, Q2 and Q3 2019 domain user access reviews performed by management, determined that: - Eight of 37 TACACS accounts were excluded from the Q2 2019 review - One terminated user was listed as part of the Q2 2019 user access review and access was not identified to be removed. Through inquiry and inspection of the evidence of the identified accounts, determined the 8 TACACS accounts were reviewed and approved during the Q3 2019 review.	CD	Y	N/a	As documented in management's response, none of the terminated users had logged into their account after their termination. The unauthorized access was removed upon detection or the error. The policy and procedures related to the error were reiterated to employees affected. Based on these factors, no impact to the SolarWinds control environment was identified.	As documented in management's response, none of the terminated users had logged into their account after their termination. The unauthorized access was removed upon detection or the error. The policy and procedures related to the error were reiterated to employees affected. Based on these factors, no impact to the SolarWinds control environment was identified.	